24. (Original) The apparatus of claim 23 wherein the physical elements comprising the system are selected from the group consisting of IP address, machine type, operating system, users, file system structure, vulnerabilities on machines, and programs running on machines.

Remarks

Invention Summary and Background Remarks Relating to the Status of the Claims

Applicants disclose and claim a computer system analysis tool and method that will allow for qualitative and quantitative assessment of security attributes and vulnerabilities in systems including computer networks. The invention is based on generation of attack graphs wherein each node represents a possible attack state and each edge represents a change in state caused by a single action taken by an attacker or unwitting assistant. Edges are weighted using metrics such as attacker effort, likelihood of attack success, or time to succeed. Generation of an attack graph is accomplished by matching information about attack requirements (specified in "attack templates") to information about computer system configuration (contained in a configuration file that can be updated to reflect system changes occurring during the course of an attack) and assumed attacker capabilities (reflected in "attacker profiles"). High risk attack paths, which correspond to those considered suited to application of attack countermeasures given limited resources for applying countermeasures, are identified by finding "epsilon optimal paths."

Claims 1 – 24 were originally filed in this Application. None of the claims have been amended.

Under the present First (non-final) Office Action all of the claims stand rejected under 35 U.S.C. 103(a) as being unpatentable over Ortalo, et al. in view of Clarkson. In response to the present Office Action, Applicants present the following argument in support of the claims as originally filed.

According to the Office, " it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Clarkson within the system of Ortalo et al., because determining the shortest path length from the attacker to the target system allows the least effort network vulnerabilities to be determined and patched so as to harden the network and prevent future similar attacks. In response, Applicants submit that the Office has failed to establish a prima facie case of obviousness, because the Ortalo, et al. reference ***teaches away*** from the combination suggested by the Office.

Specifically, according to the Office, Ortalo, et al., does not meet Applicants claimed limitations reflected in lines 21 - 26, and so the office relies on Clarkson to supply the missing information from Ortalo, et al, concerning identifying " epsilon optimal paths" defined in the claim as having a length, $L \quad (1+\varepsilon)$ times the length of the shortest path. Ortalo, et al., however, states on p. 644, col. 2, first paragraph, last sentence,

> " In fact, more than its length, its is the nature of the path and of the vulnerabilities involved that will be of interest to improve the security, as it is the path that seems to have the major impact on METF_{ML} and METF_{TM}."

Then, on p. 644, col. 2, fifth paragraphs, Ortalo, et al., states,

> " Globally, we can see that the number of paths existing between the attacker and the target is a measure that would raise a significant number of alarms, among which some may be relatively uninteresting. Moreover, not all important security events would raise an alarm. Consequently, this measure seems more difficult to use than METF$_{ML}$ and METF$_{TM}$ and it is less reliable."

Ortalo, et al. teach that, when compared with Mean Effort to Failure, path length and number of paths are not desirable criteria to consider in assessing network vulnerability. Consequently, as a result of this teaching away, one of ordinary skill in the art would not have been motivated to combine the teachings of Ortalo, et al., with the teachings of Clarkson, which do address path length, and which, according to the Office, satisfy the limitation not met by Ortalo, et al. Therefore, the Office has not established a prima facie case of obviousness with regard to Claim 1.

Similarly, with respect to Claim 12, the Office states that Clarkson satisfies the limitation in lines 25 - 31 of that claim, even though Ortalo does not meet the limitation. Once again, as a result of teaching away by Ortalo, one of ordinary skill in the art would not have been motivated to combine the teachings of Ortalo, et al., and Clarkson. Therefore, the Office has not established a prima facie case of obviousness with regard to Claim 12.

Since Claims 2 - 11 depend from Claim 1, and Claims 13 - 24 depend from Claim 12, the lack of prima facie obviousness applies to all currently pending claims. Therefore, Applicants submit that claims 1 - 24 are in condition for allowance. Reconsideration and withdrawal of the rejections as to those claims are requested. Allowance of claims 1 – 24 at an early date is solicited.

Respectfully submitted,

Russell D. Elliott
Attorney for Applicants
Registration No. 35,497
Sandia National Laboratories
P.O. Box 5800 - MS 0161
Albuquerque, NM 87185-0161
Ph. (505) 844-5626
Fax (505) 844-1418

CERTIFICATE OF MAILING (37 CFR 1.8(a))

I hereby certify that the foregoing paper (along with any paper referred to as being attached or enclosed) is being deposited with the U.S. Postal Service ion the date shown below with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: 3/22/05 Viola Campos